02:00:00

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

- - -

UNITED STATES OF AMERICA,	:	CASE NO. 1:18-cr-0043
Plaintiff,	:	
vs.	:	TRIAL EXCERPT
YANJUN XU, also known as XU YANJUN, also known as QU HUI, also known as ZHANG HUI,	:	27th of OCTOBER, 2021 9:39 A.M.
Defendant.	:	

- - -

EXCERPT OF TRANSCRIPT OF PROCEEDINGS
TESTIMONY OF ADAM ROBERT JAMES
BEFORE THE HONORABLE TIMOTHY S. BLACK, JUDGE

- - -

APPEARANCES:

For the Plaintiff:

Timothy S. Mangan, Esq.
Emily N. Glatfelter, Esq.
Assistant United States Attorneys
221 East Fourth Street, Suite 400
Cincinnati, Ohio 45202
and
Matthew John McKenzie, Esq.
United States Department of Justice
National Security Division
950 Pennsylvania Avenue NW
Washington, D.C. 20530
and
Jacqueline K. Prim
Special Assistant, Paralegal
United States Department of Justice
National Security Division
950 Pennsylvania Avenue NW
Washington, D.C. 20530

For the Defendant:

Ralph William Kohnen, Esq.
Jeanne Marie Cors, Esq.
Sanna-Rae Taylor, Esq.
Taft Stettinius and Hollister
425 East Walnut Street, Suite 1800
Cincinnati, Ohio 45202
and

Robert K. McBride, Esq.
Amanda Johnson, Esq.
Taft Stettinius and Hollister
50 East RiverCenter Boulevard
Suite 850
Covington, Kentucky 41011
and
Florian Miedel, Esq.
Miedel & Mysliwiec, LLP
80 Broad Street, Suite 1900
New York, New York 10004

Also present: Mae Harmon, Interpreter
Robin Murphy, Interpreter
Yanjun Xu, Defendant

Law Clerk: Cristina V. Frankian, Esq.

Courtroom Deputy: Rebecca Santoro

Stenographer: Mary Schweinhagen, RPR, RMR, RDR, CRR
United States District Court
200 West Second Street, Room 910
Dayton, Ohio 45402

Proceedings reported by mechanical stenography, transcript produced by computer.

*** *** *** ***

INDEX OF WITNESSES

WEDNESDAY, OCTOBER 27, 2021

* * * * *

P-R-O-C-E-E-D-I-N-G-S 3:18 P.M.

(Proceedings reported but not transcribed.)

09:39:50 THE COURT: Let's call for the jury.

09:41:30 THE COURTROOM DEPUTY: All rise for the jury.

09:41:32 (Jury in at 9:41 a.m.)

09:42:05 THE COURT: You may all be seated. Thank you. The 15 jurors have arrived. Good morning and welcome back. I told you this a couple of times; I want you to believe it deep, deep inside. The Court and the community and the participants appreciate your work.

09:42:22 We're going to continue with the testimony of this gentleman. He's still under oath.

09:42:28 The government may proceed.

09:42:31 **ADAM ROBERT JAMES, PLAINTIFF WITNESS, PREVIOUSLY SWORN**

09:42:31 MR. McKENZIE: Thank you, Your Honor. For the record, this is Matthew McKenzie for the government.

09:42:39 THE COURT: Very well. Can you orient those microphones, please.

09:42:46 MR. McKENZIE: Is this better, Your Honor?

09:42:48 THE COURT: A little bit.

09:42:52 MR. McKENZIE: I will try to keep my voice up.

09:42:54 THE COURT: That's perfect.

09:42:56 **DIRECT EXAMINATION (CONT.)**

09:42:56 BY MR. McKENZIE:

09:42:56 **Q.** Speaking of reorienting, Special Agent James, I'd like to

direct your attention to the forensic analysis that you conducted of the hard drive that we discussed yesterday.

You mentioned a type of malware that you found called Sakula. Remind the jury what type of malware Sakula is.

A. Sakula is a remote access trojan that beacons to the Internet.

Q. Do remote access trojans, are they a type of trojan horse?

A. They are.

Q. And please remind us, on what date was the Sakula malware installed on the hard drive you analyzed?

A. January 25th of 2014.

MR. McKENZIE: Your Honor, I ask that we publish Government's Exhibit 110 on page 1 -- on page 3.

THE COURT: It's been admitted?

MR. McKENZIE: Which has been admitted, yes.

THE COURT: Yes, you may publish it.

And if the special agent would keep his voice up, please.

THE WITNESS: Yes, sir.

MR. McKENZIE: I apologize. Page 4. My mistake.

BY MR. McKENZIE:

Q. Just to again get us reoriented, directing your attention to the first message sent on January 25, 2014, will you please read that message?

A. "The horse is planted. This morning."

09:44:40 **Q.** Who sent that message.

09:44:42 **A.** Tian Xi.

09:44:46 MR. McKENZIE: To refresh our recollection on who Tian Xi is, may I please publish Government's Exhibit 111, page 6, which is in evidence?

09:45:06 THE COURT: Yes.

09:45:06 BY MR. McKENZIE:

09:45:06 **Q.** Directing your attention to the top right column, do you see the name Tian Xi?

09:45:12 **A.** I do.

09:45:12 **Q.** Directing your attention to the first sentence of the first full paragraph, does it identify Tian Xi as a manufacturing engineer?

09:45:25 **A.** It does.

09:45:28 MR. McKENZIE: Okay. I would like to return one more time to Government's Exhibit 110, page 4?

09:45:38 THE COURT: Yes.

09:45:45 BY MR. McKENZIE:

09:45:45 **Q.** Directing your attention to the first message of January 25, 2014, to whom did Tian send that message?

09:45:52 **A.** Xu Yanjun.

09:46:02 **Q.** Okay. I think we are now back to where we were yesterday.

09:46:04 I'd like to return to your forensic analysis. Yesterday you discussed the Sakula malware, but you also mentioned a

09:46:14 second type of malware that you discovered. Will you remind
09:46:17 us what that program is called?
09:46:19 **A.** That program is called plugX.
09:46:22 **Q.** How many types of variants of plugX did you find on
09:46:28 the -- on the hard drive?
09:46:28 **A.** There were two different versions of plugX on the hard
09:46:33 drive.
09:46:33 **Q.** Will you explain to the jury what it means to have
09:46:37 multiple versions of plugX?
09:46:43 **A.** What it means to have multiple versions of plugX is
09:46:46 there are actually two sets of files related to the plugX
09:46:50 malware that were independent of each other.
09:46:54 **Q.** Did you analyze both sets of files?
09:46:56 **A.** I did.
09:46:57 **Q.** Did both of them work?
09:46:58 **A.** No, they did not both work.
09:47:01 **Q.** Tell the jury what you mean by that.
09:47:03 **A.** So the plugX malware is composed of several different
09:47:10 files that it needs to have in order to operate correctly.
09:47:14 One of the variants of plugX, one of the files appeared to
09:47:19 be corrupted, and so it did not run properly when you
09:47:23 attempted to run it. Or when I attempted to run it.
09:47:27 **Q.** And what about the other variant of plugX? Did that
09:47:31 work?
09:47:32 **A.** The other variant did work properly.

09:47:34 **Q.** What type of malware is plugX?

09:47:37 **A.** PlugX is a remote access trojan.

09:47:41 **Q.** And what happened when you ran the variant of plugX that worked?

09:47:45 **A.** The variant that successfully ran would issue a beacon to a domain on the Internet.

09:47:52 **Q.** Were you able to determine what that domain was?

09:47:55 **A.** I was.

09:47:55 **Q.** And what was that domain?

09:47:58 **A.** The domain for the variant of plugX that worked was ns24.dnsdojo.com.

09:48:12 **Q.** Do you sometimes refer to that as dnsdojo.com?

09:48:17 **A.** I do.

09:48:19 **Q.** What does it mean in plain English that the program beaconed to this dnsdojo.com?

09:48:27 **A.** The beacon to dnsdojo.com was a way for the malware to check in with the computer intruders that intended to control it.

09:48:38 **Q.** Based on your analysis of the hard drive, did the plugX program actually beacon out to dnsdojo.com?

09:48:49 **A.** From my analysis of the hard drive, I could not determine that.

09:48:51 **Q.** Were you able to determine that it was designed to do so?

09:48:55 **A.** Yes.

09:48:56 **Q.** Are you familiar with the term "Crowd Strike"?

09:49:02 **A.** I am.

09:49:03 **Q.** What is Crowd Strike?

09:49:05 **A.** Crowd Strike is a US information security and incident response company.

09:49:10 **Q.** Does Crowd Strike publish publicly available blog posts about hacking activities?

09:49:18 **A.** They do.

09:49:18 **Q.** Directing your attention to on or about February 25, 2014, did there come a time that you became aware of a blog post on Crowd Strike?

MS. CORS: Your Honor, objection.

THE COURT: Basis?

MS. CORS: Hearsay.

MR. McKENZIE: I haven't gotten into the substance of anything yet.

THE COURT: We are not there yet. Overruled.

BY MR. McKENZIE:

Q. Did you become aware of a blog post on Crowd Strike?

A. I was aware that there was a blog post.

Q. Without getting into the details, what was the general topic of the post?

A. The general topic of the post was computer intrusion activity targeting French aerospace.

Q. Was that post published on the Internet?

A. It was.

09:50:07 **Q.** I'd like to direct your attention back to Government's
09:50:12 Exhibit 110, page 4. And I'd like to begin with the messages
09:50:28 on February 25, 2014. Will you please read just the first
09:50:34 message?
09:50:35 **A.** "Call me back as soon as possible."
09:50:40 **Q.** Who sent that message?
09:50:41 **A.** Xu Yanjun.
09:50:45 **Q.** To whom did he send it?
09:50:47 **A.** Chai Meng.
09:50:50 **Q.** On what date was this message sent?
09:50:52 **A.** February 25th of 2014.
09:50:56 **Q.** On what date did Crowd Strike publish the blog post about
09:51:01 hacking activities targeting French aerospace?
09:51:05 **A.** February 25th of 2014.
09:51:08 **Q.** I'd like to read the remaining messages on the page. I
09:51:13 will read the messages sent by Chai Meng.
09:51:20 So please read the next message.
09:51:23 **A.** "What does Chen mean?"
09:51:24 **Q.** "Chen is still reporting, and I'm waiting for him to come
09:51:27 out."
09:51:28 **A.** "Ah. How will Chen Li react to this matter? The mail
09:51:34 has been forwarded to your email address."
09:51:39 MR. McKENZIE: Could we please go to page 5?
09:51:42 THE COURT: Yes.
09:51:46 BY MR. McKENZIE:

09:51:46 **Q.** Let us continue with the next two messages.

09:51:52 "Okay."

09:51:53 **A.** "The part with the red marking in the attachment, is that being flagged by Suzhou's investigation?"

09:52:05 **Q.** Who sent that last message?

09:52:08 **A.** Xu Yanjun.

09:52:10 **Q.** To whom did he send it?

09:52:12 **A.** Chai Meng.

09:52:13 **Q.** Where is Safran Suzhou located?

09:52:20 **A.** In Suzhou.

09:52:22 **Q.** And who is the parent company of Safran Suzhou?

09:52:27 **A.** Safran Group.

09:52:31 **Q.** What company owns the computer that you analyzed?

09:52:35 **A.** Safran.

09:52:37 **Q.** In what company -- in what country is Safran located?

09:52:40 **A.** They are located in France.

09:52:44 **Q.** Will you please read the next message.

09:52:48 **A.** "Your QQ."

09:52:50 **Q.** Do you know what "QQ" stands for or what "QQ" is?

09:52:54 **A.** I do.

09:52:55 **Q.** What is QQ?

09:52:56 **A.** QQ is -- the most common thing it's used for is a mobile messaging app.

09:53:05 **Q.** Is it popular in China?

09:53:07 **A.** It is.

09:53:08 **Q.** We will go through these messages. I will read Song
09:53:16 Sicheng. He responded with a series of numbers.
09:53:21 Please read the next message.
09:53:23 **A.** "Received. Sent already."
09:53:27 **Q.** "Okay. I am receiving it."
09:53:31 Directing your attention to the next set of messages,
09:53:35 will you please read the -- just the next message?
09:53:39 **A.** "What does Chen mean by heaping the responsibility upon
09:53:43 me and furthermore having the guest to find Gu?"
09:53:50 **Q.** Who sent that message?
09:53:51 **A.** Xu Yanjun.
09:53:53 **Q.** To whom did he send it?
09:53:56 **A.** Chai Meng.
09:53:56 **Q.** All right. We will read the next exchange. I will read
09:53:59 the parts of Chai Meng. Please read the next message.
09:54:02 **A.** "Isn't it like putting a noose on his own neck?"
09:54:06 **Q.** "I don't know. I told him the French device was seized.
09:54:09 He immediately stated that he had foresight. As to matter of
09:54:16 finding Gu, he never told me about it."
09:54:20 Let's pause there for a moment.
09:54:27 What country did the hard drive you analyzed come from?
09:54:30 **A.** It came from France.
09:54:36 **Q.** I'd like to take a pause from Government's Exhibit 110
09:54:39 and turn to Government's Exhibit 111, page 1.
09:54:49 Directing your attention to the top of the screen next to

"Name," will you please read the name?

A. Gu Gen.

Q. Scrolling down to the middle of the page where it says "Position," will you please read the position?

A. "Senior IT infrastructure manager and information security officer."

Q. Scrolling to the bottom of the screen underneath the red seal, will you please read the company?

A. "Safran Beijing Enterprise Management Company, Ltd., Suzhou Branch.

Q. Thank you.

MR. McKENZIE: I'd like to return to Government's Exhibit 110, which is in evidence. I believe we were on page 5.

THE COURT: Very well.

BY MR. McKENZIE:

Q. Directing your attention to the message sent at 3:10 p.m. We'll continue reading with you reading the part of Xu Yanjun and I'll read Chai Meng.

A. "I wanted to call him a son of a bitch. He stated the entire thing led to an exposing is because what the guest has planted in the French device."

Q. In the term or in the context of a cyber intrusion case, what does "planted" mean?

A. To install.

09:56:12 **Q.** All right. The next message was sent at 3:12 p.m.

09:56:16 "It's my guess to prove his brilliance."

09:56:20 **A.** "It feels bitterly disappointing to have leaders like that."

09:56:24

09:56:25 "Can you suggest not letting the guest go to find Gu? First, the guest is not exposed; two, Gu doesn't have the power to decide. Thirdly, Gu would report the situation to me at any time."

09:56:34

09:56:37

09:56:40

09:56:43 **Q.** We will continue on to the first message from February 26, 2014. Will you please read the first message?

09:56:49

09:56:54 **A.** "France is letting Little Gu to check out this record, ns24.dnsdojo.com. Does it have anything to do with you all?"

09:57:00

09:57:07

09:57:08 **Q.** Who sent that message?

09:57:09 **A.** Xu Yanjun.

09:57:10 **Q.** To whom did he send it?

09:57:12 **A.** Chai Meng.

09:57:13 **Q.** In what country is Safran located?

09:57:16 **A.** They are located in France.

09:57:18 **Q.** Who did Gu Gen work for?

09:57:21 **A.** Safran Suzhou.

09:57:23 **Q.** To what domain did the plugX malware you found on the hard drive beacon?

09:57:27

09:57:28 **A.** Ns24.dnsdojo.com.

09:57:38 **Q.** At 3:08 Chai Meng responded, "Let me ask."

Directing your attention to the next message sent on February 27, 2014, will you please read that message?

A. "France is asking Little Gu to inspect this record, ns24.dnsdojo.com. Is it related to you?"

Q. To what domain did the plugX malware beacon?

A. Ns24.dns.dojod.com.

Q. Directing your attention back to Government's Exhibit 111, page 1.

MR. McKENZIE: And if I may publish to the jury, Your Honor.

THE COURT: Yes. It's been admitted, right?

MR. McKENZIE: Yes, Your Honor.

BY MR. McKENZIE:

Q. Scrolling down to "Position." Will you read Gu Gen's position?

A. The senior IT infrastructure manager and information security officer.

Q. Based on your years of experience in information technology and security and work in cyber intrusion investigations, what is the role of senior IT and security officers in investigating cyber intrusions for a company?

A. Generally, your information security office would be the office that conducts computer or -- well, intrusion, computer intrusion investigations into the company.

Q. I'd like to direct your attention back to Government's

Exhibit 110, page 5, which is in evidence.

I'd like to move on now to the message sent on -- the messages sent on March 11, 2014. Will you please read the first message?

A. "When did Gu ask you? When did France ask you?"

Q. Who sent that message?

A. Xu Yanjun.

Q. To whom did he send it?

A. Tian Xi.

Q. I will read the messages sent by Tian Xi.

"Gu received an email from the French side, asked me yesterday."

A. "Have you seen the email?"

Q. "No."

What country is Safran located in or headquartered in?

A. They are headquartered in France.

Q. Could we please see the next page.

For March 17th, will you please read the messages sent by Xu Yanjun, and I will read the messages sent by Tian Xi?

A. "Anything new? I sought out Little Gu last week and current France has not finding suspicious documents in the record."

Q. "Nothing."

A. "Should there be something new be prompt notifying me and I will communicate with Little Gu."

10:01:03 **Q.** "Understand."

10:01:04 Directing your attention now to April 17, 2014, messages, let's read the first three messages, you reading those sent by the defendant, I'll read those sent by Tian Xi.

10:01:18 **A.** "Of the matter, any new situation?"

10:01:21 **Q.** "No."

10:01:23 **A.** "Good."

10:01:28 **Q.** Directing your attention to the next message that was sent, will you please read the message?

10:01:33 **A.** "Any updates on that incident?"

10:01:37 **Q.** Who sent the message?

10:01:38 **A.** Xu Yanjun.

10:01:40 **Q.** To whom did he send it?

10:01:41 **A.** Gu Gen.

10:01:43 **Q.** Who does Gu Gen work for?

10:01:46 **A.** Safran Suzhou.

10:01:47 **Q.** I will read Gu's response.

10:01:52 "Still checking. They found that someone had connected to our server via a tool called psexec. The period is from July last year to February this year."

10:02:02 Will you please read the next message?

10:02:04 **A.** "No conclusion?"

10:02:08 **Q.** Directing your attention to the next message, the second message sent at 9:46 a.m., will you please read that message?

10:02:17 **A.** The latest status from Suzhou: They found an intrusion

10:02:22 to our server through a psexec tool. The time frame is from
10:02:28 July last year to February this year."
10:02:31 **Q.** Who sent that message?
10:02:33 **A.** Xu Yanjun.
10:02:35 **Q.** To whom did he send it?
10:02:37 **A.** Chai Meng.
10:02:38 **Q.** And what is the location of Safran's subsidiary in China?
10:02:41 **A.** Suzhou.
10:02:42 **Q.** Directing your attention to the next message sent at 9:55
10:02:53 a.m., did Gu Gen send a message to the defendant which said,
10:02:59 "So far, no. They will examine by remotely connecting to this
10:03:02 server"?
10:03:06 **A.** He did.
10:03:06 **Q.** How did the defendant respond?
10:03:08 **A.** "Do they think China is hacking them?"
10:03:12 **Q.** And will you please read Gu's response?
10:03:15 **A.** "Don't think so."
10:03:18 **Q.** Directing your attention now to the messages sent on
10:03:22 August 18, 2014. Who sent the first message that we see on
10:03:28 that date?
10:03:29 **A.** Xu Yanjun.
10:03:31 **Q.** To whom did he send it?
10:03:32 **A.** Tian Xi.
10:03:34 **Q.** Please read the defendant's messages. I'll read Tian's
10:03:37 response.

10:03:38 **A.** "About that matter, any new situation?"

10:03:41 **Q.** "No new news. Should be an unsolved mystery."

10:03:50 **A.** "Ho, ho."

10:03:51 MR. McKENZIE: For a final time, I would like to return to Government's Exhibit 111, page 1, which is in evidence, Your Honor.

10:04:01 BY MR. McKENZIE:

10:04:04 **Q.** Will you please read the title of the document which is displayed at the top of the screen?

10:04:11 **A.** "Employment Dismissal Record Form for Employers of Suzhou Industrial Park."

10:04:20 **Q.** Please read the name that's listed at the top of the screen.

10:04:23 **A.** Gu Gen.

10:04:26 **Q.** Scrolling down and directing your attention to the middle of the screen, what was Gu's position?

10:04:32 **A.** Senior IT infrastructure manager and information security officer.

10:04:40 **Q.** When it says "Type of" -- directing your attention to the box below it, next to "Type of Contract Dissolution (Termination)," which box has been selected?

10:04:52 **A.** The box for "Employer Initiated Dissolution" is highlighted.

10:04:59 **Q.** Scrolling down, who is listed as the employer?

10:05:05 **A.** Safran Beijing Enterprise Management Company, Ltd.,

10:05:10 Suzhou Branch.
10:05:12 **Q.** And directing your attention to that same box, what is
10:05:15 listed as the date?
10:05:16 **A.** November 28 of 2018.
10:05:18 **Q.** I'd like to direct your attention now to page 6 of the
10:05:21 same exhibit.
10:05:30 Directing your attention to the top left. Who is the
10:05:34 sender of this letter?
10:05:34 **A.** Safran Aircraft Engines, Suzhou Co., Ltd.
10:05:41 **Q.** Who is the recipient of the letter?
10:05:43 **A.** Tian Xi.
10:05:45 **Q.** In the -- in that same column, what is the date of the
10:05:50 letter?
10:05:53 **A.** It appears to be November 13th of 2018.
10:05:57 **Q.** As displayed on the screen currently to your bottom left,
10:06:02 what is the title of this letter?
10:06:05 **A.** "Re: Termination Letter."
10:06:08 MR. McKENZIE: If we can scroll down to where we can
10:06:12 begin with "Dear Sir."
10:06:12 BY MR. McKENZIE:
10:06:14 **Q.** Will you please read the English section of this letter?
10:06:19 **A.** "Dear Sir,
10:06:21 "Following our meeting on October 31, 2018, the company
10:06:26 has decided to dismiss you from your position of
10:06:31 manufacturing engineer. This decision is justified by the

following reasons:

"You have materially breached the employer's rules and regulation. Therefore, the company hereby terminates your employment contract in accordance with its Article 7 and PRC applicable laws, including Article 39 of the Labor Contract Law of the PRC. Your employment contract entered with the company on December 10, 2007, will terminate with immediate effect. Therefore, you will leave the company on November 13, 2018.

"In consideration of the above, the company will not pay you any compensation.

"Before leaving the company, please surrender any and all relevant work, documents, equipment, and property, together with all keys, relating to the company and/or any of its clients to Patrick Calero.

"As from the date of the termination of your employment, you will remain bound by the confidentiality undertaking stipulated in your employment contract which stipulates that you shall keep strictly secret and confidential, and not disclose to any third party any and all technical, economic, financial, or marketing information acquired from the company and/or obtained because of your activities in the company.

"The company reserves all rights to bring suits, claims, or any other actions against you.

10:08:17 "Yours sincerely."

10:08:19 **Q.** And then what is -- who is listed as the company sending the letter?

10:08:23 **A.** Safran Aircraft Engines, Suzhou Co., Ltd.

10:08:32 THE COURT: Counsel, I'd like to take a break at an appropriate point.

10:08:34 MR. McKENZIE: Perfect timing, Your Honor. The government has no further questions.

10:08:35 THE COURT: Very well. We are going to recess for 20 minutes, until 10:30.

10:08:40 Members of the jury, as you know, please do not discuss the case among yourselves or with anyone else. No independent research. Continue to keep an open mind.

10:08:47 We'll rise as you leave.

10:08:50 THE COURTROOM DEPUTY: All rise for the jury.

10:08:54 (Jury out at 10:09 a.m.)

10:09:00 THE COURT: Jury's left the room and the door is closed. We're going to break until 10:30, at least as to the jury. That's my intention.

10:09:02 We can chat in 15 minutes or the issues that are arising may not require attention yet. When is the witness to be called that Mr. --

10:09:03 THE INTERPRETER: Your Honor, the interpreter is having a hard time hearing you. I'm sorry.

10:09:43 THE COURT: That's okay.

10:09:45

10:09:48

10:09:51

10:09:59

10:10:03

10:10:08

10:10:09

10:10:13

10:10:19 Do I need to address the defense's concerns about Arthur
10:10:24 Gau now from the government's perspective?
10:10:28 MR. MANGAN: He is the next witness. It's a matter
10:10:30 of whether you wanted to wait until the next break or not.
10:10:35 We're fine either way.
10:10:36 THE COURT: Why don't we be seated and hear the
10:10:38 issue. We're outside the presence of the jury. We're talking
10:10:43 about the next witness.
10:10:46 Mr. Miedel, forget my lapse. I know exactly who you are.
10:10:52 MR. MIEDEL: You can just keep calling me the New
10:10:56 York lawyer. That's okay.
10:10:57 THE COURT: If you can take the mask off and tell me
10:11:00 what I can call you.
10:11:02 MR. MIEDEL: The New York lawyer.
10:11:03 THE COURT: I didn't want to do that.
10:11:06 MR. MIEDEL: Your Honor, I wanted to raise this
10:11:07 issue because, as I said, Arthur Gau is the next witness. And
10:11:10 according to the government's exhibit book, they, I think,
10:11:16 will attempt to introduce Exhibit 81a and 81b through Arthur
10:11:22 Gau.
10:11:26 Exhibit 81 is a Chinese letter, in Chinese, and 81b is
10:11:33 the English translation of it. And it essentially is a typed
10:11:37 letter that Arthur Gau will testify was given to him in 2003,
10:11:44 purportedly by an individual named Zha, Z-H-A, Rong, R-A-N-G
10:11:51 [sic], who I think the government will argue was somehow

10:11:53 associated with MSS, or at least later was.

10:11:58 And that letter contains a number of questions about what
10:12:04 seemed to be engineering questions or problems. We object to
10:12:12 the introduction of that exhibit for a couple of reasons. The
10:12:15 first is that it is hearsay. It is an out-of-court statement
10:12:21 obviously made, proposed for the truth of the matter because
10:12:25 the government wants to show that the document is asking
10:12:29 Arthur Gau specific engineering questions or presents
10:12:36 engineering issues that they want him to respond to.

10:12:41 There is no applicable hearsay exception because this
10:12:44 letter was created and given to Arthur Gau ten years before
10:12:49 the beginning of the conspiracy in this case. It was given in
10:12:53 2003. The conspiracy begins, according to the indictment, in
10:12:58 2013.

10:13:00 And if it's not being introduced for the truth, then it
10:13:04 has no relevance, because if it is not for purposes of the
10:13:09 charged conspiracy, the letter itself does not ask for any
10:13:14 specific trade -- it doesn't ask for the -- Mr. Gau to reveal
10:13:21 trade secrets. As noted, it was written 10 years before the
10:13:25 conspiracy. At that point in 2003, Mr. Xu was not involved in
10:13:30 that. There is no evidence that he was even working with Zha
10:13:39 Rong at that time. There is no evidence that Zha Rong was
10:13:42 working for MSS at the time. Arthur Gau will testify,
10:13:46 presumably, that he believe that Zha Rong was working for
10:13:50 NUAA.

10:13:52 In terms of relevance, it is absolutely more prejudicial
10:13:59 than probative, again because -- the probative value is
10:14:04 minimal again because it occurred ten years before the charged
10:14:08 conspiracy.
10:14:09 The document is signed by Zha Rong -- it's typed, so it's
10:14:16 not signed but it's typed with his name, but we don't actually
10:14:20 have any way of knowing who wrote it. It was not given to
10:14:23 Arthur Gau by Zha Rong; it was given to him by somebody else.
10:14:28 The document doesn't actually ask him to reveal any trade
10:14:32 secrets.
10:14:32 And I think that what the problem is, the prejudice is
10:14:35 that the jury could mistakenly conclude that this was a
10:14:41 decades-long pattern in an effort to get Mr. Gau to cough up
10:14:50 trade secrets when, in fact, there is -- this document doesn't
10:14:52 advance that theory at all. And the jury could mistakenly
10:14:55 consider it to be meaningful when it's not. Thank you.
10:15:01 THE COURT: When did this issue -- when did you
10:15:05 become aware of it?
10:15:07 MR. MIEDEL: Well, I was aware of it for a while
10:15:10 but, again, Mr. Gau wasn't scheduled to be testifying until
10:15:15 today. So I notified the government of it this morning. I
10:15:18 think they are prepared to argue it.
10:15:19 THE COURT: The Court prefers to get a heads-up.
10:15:25 MR. MIEDEL: I understand.
10:15:26 THE COURT: The government wish to be heard?

10:15:28 MR. MANGAN: Yes, Your Honor. What I would say in
10:15:34 response is, first of all, this does pertain to an individual
10:15:39 named Zha Rong, and there's already been evidence submitted in
10:15:42 the case relating to Mr. Zha Rong and his relationship to the
10:15:46 defendant. As we've asserted, he is the direct supervisor of
10:15:51 the defendant within the MSS.
10:15:59 What we are going to go through with Arthur Gau is a
10:16:02 number of trips that he took over to China and that he met
10:16:04 with Zha Rong on a number of those trips and then eventually
10:16:08 was introduced to the defendant.
10:16:10 And so our assertion, Your Honor, is that the
10:16:13 relationship started with Zha Rong. It was more or less
10:16:16 passed over to the defendant, to kind of continue with the
10:16:21 relationship in later visits, and that will be the heart of
10:16:24 the testimony, will be these later visits. However, to
10:16:27 explain sort of where it all started, his first visits were,
10:16:32 you know, back in that time period, when he went back to China
10:16:37 in, you know, the year 2000 and so on.
10:16:39 When he got back to the U.S. after one of these visits
10:16:42 where he met with an NUAA professor and he met with Zha Rong,
10:16:49 at that time the son of the professor showed up at Mr. Gau's
10:16:52 house in the U.S. and handed him this letter. So in the
10:16:57 letter it is written and signed by Zha Rong asking him to see
10:17:04 if he's willing to do a project that would prepare a lot of
10:17:06 technical information.

10:17:08 So from our standpoint, Your Honor, there is two things.
10:17:11 One, to the extent it is simply a question or it is asking him
10:17:16 to do work and setting forth what they are asking for, that is
10:17:19 not hearsay. It's simply a question or it's a request or a
10:17:24 demand. Those are not assertions of fact.
10:17:29 In addition, Your Honor, to the extent any of the letter
10:17:31 would be interpreted as an assertion of fact, we would assert
10:17:35 that statements by Mr. Zha Rong are statements of a
10:17:43 co-conspirator and therefore also would be admissible.
10:17:46 As to the time frame, Your Honor, this is really -- we
10:17:48 understand we are limited by the years in the indictment
10:17:51 regarding the defendant's conduct. And that is from 2013, you
10:17:56 know, to the time of his arrest. This is kind of introductory
10:18:01 evidence to help the witness explain where the relationship
10:18:06 started and, you know, then ultimately explain where it went
10:18:11 in the years of 2016 through 2017.
10:18:16 THE COURT: So how is the letter necessary? Why
10:18:18 can't Gau just explain the origins of their relationship?
10:18:22 MR. MANGAN: He can, Your Honor. What we wanted to
10:18:26 also bring out was that at one point Zha Rong did make an ask
10:18:32 for him to do technical work that he had declined. And then
10:18:38 there is a break in time, and then the relationship is
10:18:40 restarted. So we did see some significance in that.
10:18:48 MR. MIEDEL: Your Honor, may I respond?
10:18:49 THE COURT: Yes, you get the reply.

10:18:52 MR. MIEDEL: A couple things. First of all, while
10:18:54 the government has some evidence that Zha Rong worked with
10:18:57 Mr. Xu or was his supervisor in, I don't know, 2015, 2016,
10:19:02 that's 13 years after this letter. There is zero evidence
10:19:05 that Zha Rong worked with Mr. Xu in 2003.
10:19:09 Secondly, to the extent that the government is simply
10:19:13 suggesting that this letter asked for, quote, technical work,
10:19:18 that's irrelevant. The issue at this trial is whether Mr. Xu
10:19:23 conspired or attempted to gain trade secrets, not technical
10:19:27 work. But it is -- and so there is a ten-year gap between any
10:19:35 correspondence between Mr. Gau in 2003 and Mr. Zha Rong in
10:19:40 2003 and the next time that they talk. So the suggestion that
10:19:43 there is some sort of pattern or a beginning of a relationship
10:19:47 is simply belied by -- will be belied by the testimony of
10:19:51 Mr. Gau. There was no contact between them for a decade. And
10:19:55 so it is simply way outside the scope of the conspiracy. It
10:20:00 cannot -- you cannot be a co-conspirator outside the scope of
10:20:05 the conspiracy. And so it's just, I think, improper to admit
10:20:11 this document.
10:20:11 And I think -- I agree with Your Honor that Mr. Gau can
10:20:15 certainly talk about his visits to China in 1997 and 2000 and
10:20:19 2002 and who he met there if he wants, but the introduction of
10:20:24 this document is prejudicial.
10:20:32 THE COURT: The Court sustains the defendant's
10:20:35 objection. What Zha Rong may have been doing in 2003 is not

relevant, the background as to how Mr. Gau came to be involved with the defendant, and he can explain that, he can explain, I suppose, that he knew Zha Rong in 2003 and later met the defendant.

If the defendant on cross questions Gau's explanation of how he initially came to meet Zha Rong and, later, defendant, then, by all means, the letter would start to become relevant. But as an initial matter, Gau can explain it as an initial matter without the letter, and the objection is sustained.

We're going to go into our recess unless there is something else I need to address outside the presence of the jury at this moment. Is there from the government?

MR. MANGAN: No, Your Honor.

THE COURT: The defense?

MR. MIEDEL: No, Your Honor. Thank you.

THE COURT: We're in recess.

THE COURTROOM DEPUTY: All rise. This court's now in recess.

(Recess from 10:21 until 10:41 a.m.)

THE COURT: Back in the courtroom late. The jury's not yet here.

We've had some drama. When my daughters used to live at home with my wife and me, we had drama every day. I am well trained in drama. It arises out of primarily the fact that the second interpreter who had joined us today has indicated

10:42:21 that she typically translates hospital proceedings and does
10:42:27 not feel that she is adequately trained to assist us in a
10:42:33 courtroom that's intimidating with a bunch of lawyers. And I
10:42:39 appreciate her speaking the truth, and I have released her.
10:42:43 That means we're going to have to go in chunks as we've
10:42:47 been doing previously. We're going to work as hard as we can
10:42:51 to get a second one because the current interpreter is
10:42:59 whipped. But she has agreed with me that she will take a deep
10:43:05 breath out of recognition that we're going to take short
10:43:08 breaks.
10:43:10 So we can call for the jury now.
10:44:32 THE COURTROOM DEPUTY: All rise for the jury now.
10:44:34 (Jury in at 10:44 a.m.)
10:45:06 THE COURT: You may all be seated. The 15 jurors
10:45:09 have rejoined us.
10:45:11 And I kept you waiting again. And I apologize for that.
10:45:18 I hate that. My mother would be all over me if I were keeping
10:45:24 a bunch of important people waiting. But there are times when
10:45:28 you leave that I have to address stuff that I need to deal
10:45:31 with outside your presence. The long break here had nothing
10:45:36 to do with any of the lawyers or the parties. I had to deal
10:45:39 with something. It's on me. I hope you will forgive me.
10:45:45 So we will continue with testimony. Redirect, is that
10:45:52 right?
10:45:52 MR. McKENZIE: Cross-examination at this time, Your

Honor.

THE COURT: Cross-examination.

MS. CORS: Thank you, Your Honor.

THE COURT: You may approach.

The witness remains under oath. The attorney for the defense has an opportunity to ask questions.

MS. CORS: Thank you, Your Honor. And if I go too fast, I assume someone will let me know to slow down so that the interpreter can keep up.

THE COURT: You better believe it.

CROSS-EXAMINATION

BY MS. CORS:

Q. Good morning, Special Agent. How are you today?

A. I'm good. How are you?

Q. Good.

Over the past couple days you have been asked to read from a number of text messages involving Mr. Xu, correct?

A. I have.

Q. And were these documents that you obtained through any forensic analysis you conducted?

A. The text messages were not.

Q. Okay. Where did you get those text messages from?

A. I received them from the search warrant data from the Cincinnati -- Cincinnati case.

Q. And you testified regarding your background in cyber

10:47:07 counterintelligence, correct? And computer security, and
10:47:14 explained to the jury much of the education you have had
10:47:19 relating to computers.
10:47:20 Do you have any training as an engineer?
10:47:22 **A.** I do not have any training as an engineer.
10:47:24 **Q.** And any training in the aviation field?
10:47:27 **A.** I do not.
10:47:28 **Q.** Okay. Thank you.
10:47:34 Now, you have testified about events in Suzhou relating
10:47:44 to what I believe you described as the insertion of a USB
10:47:49 drive into a computer in January of 2014, correct? January
10:47:55 25, 2014?
10:47:57 **A.** Yes.
10:47:58 **Q.** Okay. What I'd like to do is walk through the timeline
10:48:03 of events that you've testified to. So as I understand it, on
10:48:11 January 25, 2014, a USB was inserted into the computer of
10:48:20 Mr. Hascoet, correct?
10:48:22 **A.** That is correct.
10:48:22 **Q.** And that occurred in, you believe and have testified, his
10:48:27 office in Suzhou; is that correct?
10:48:29 **A.** I don't know where it was inserted physically.
10:48:32 **Q.** Okay. So you don't know where it was inserted. But at
10:48:38 some point on that date, based on your forensic analysis, this
10:48:43 USB drive was inserted into his computer. Is that fair?
10:48:46 **A.** That is correct.

10:48:47 **Q.** And you testified that on that same day, from that USB
10:48:55 drive, a certain virus malware was placed on the computer of
10:49:02 Mr. Hascoet, correct?
10:49:02 **A.** That is correct.
10:49:03 **Q.** And then I believe you testified that shortly thereafter
10:49:08 you read some text messages, I believe it was maybe the day
10:49:11 after, where there were communications about someone looking
10:49:16 at that computer, correct?
10:49:17 **A.** That is correct.
10:49:18 **Q.** And can you explain to the jury again what that meant to
10:49:23 you?
10:49:23 **A.** What that means to me is somebody verified that the
10:49:27 computer had beaconed in, and they would have had the
10:49:30 ability to look at files on the computer if they wanted to.
10:49:34 **Q.** So in or around the 25th, 26th, based on your review of
10:49:41 that computer and what happened with that malware and the
10:49:45 beaconing, it's your understanding that at that point in time
10:49:49 someone who had access to this server, wherever it was, would
10:49:52 have had the ability to access the computer of Mr. Hascoet,
10:49:58 correct?
10:49:58 **A.** That is correct.
10:49:59 **Q.** And that would include looking at items on the computer;
10:50:03 is that correct?
10:50:03 **A.** That is correct.
10:50:05 **Q.** Okay. And I believe you mentioned that would also

10:50:08 provide access to upload or download documents; is that
10:50:12 correct?
10:50:12 **A.** Upload or download files.
10:50:17 **Q.** Files, okay.
10:50:18 **A.** Yes.
10:50:19 **Q.** And I believe, based on your testimony, that that laptop
10:50:22 became connected to that server, I think, around the 27th of
10:50:25 January of '14. Does that sound correct to you?
10:50:29 **A.** There was evidence on the hard drive that it -- the
10:50:33 Sakula malware connected outbound as of that date.
10:50:37 **Q.** And that was to that domain you were talking about
10:50:39 earlier; is that correct?
10:50:42 **A.** Yes, that's correct.
10:50:43 **Q.** And what was that domain again?
10:50:44 **A.** There was two domains. One was oa.ameteksen.com, and
10:50:54 the other one was secure.safran-group.com.
10:51:01 **Q.** And then on or around January 30th, was that when, based
10:51:05 on your forensic analysis, some additional malware virus, the
10:51:11 key logger, was installed on that computer?
10:51:13 **A.** I believe that is correct.
10:51:14 **Q.** Okay. And at the time -- strike that. Then near the end
10:51:26 of January, around January 31, 2014, I believe in your report
10:51:33 there is an indication that the computer starts communicating
10:51:35 with secure.safran-group.com; is that correct?
10:51:41 **A.** The computer would have continued to communicate to

10:51:45 that domain, yes.
10:51:46 **Q.** Okay. So it continues to communicate, continues to
10:51:48 provide access. Whoever has access to that domain has access
10:51:52 to Mr. Hascoet's computer, correct?
10:51:53 **A.** That would be correct.
10:51:54 **Q.** Okay. And then when did that computer, from your
10:52:00 recollection, stop communicating with that domain?
10:52:09 **A.** Based on the evidence available on the hard drive, I
10:52:12 believe it was on or about February 20 -- February 14th, if
10:52:17 I remember correctly.
10:52:18 **Q.** Okay. So the computer stops communicating around
10:52:21 February 14th with this domain. And then at the same time,
10:52:26 does the key logger stop recording or was that a little later?
10:52:31 **A.** I would have to go back and look at the key logger data
10:52:37 to see when the key logger stopped.
10:52:39 **Q.** About around the same time, is it your recollection?
10:52:42 **A.** It would probably be around the same time.
10:52:45 **Q.** Okay. I think I've seen February 17, 2014?
10:52:48 **A.** Okay.
10:52:48 **Q.** Does that sound --
10:52:49 **A.** Yeah, that sounds correct.
10:52:50 **Q.** Okay. So from January 25th, we know that, based on your
10:52:56 forensic analysis, malware is put on this computer, we know
10:53:00 that the computer starts communicating with a domain, and we
10:53:04 know that that communication stops on or around February 14th,

10:53:10 correct?
10:53:10 **A.** That's --
10:53:13 **Q.** So three to four weeks, correct?
10:53:15 **A.** Yep.
10:53:16 **Q.** And based on your analysis, at any point during that time
10:53:19 was an effort made to target any documents on that computer?
10:53:22 **A.** Based on the evidence on the hard drive? It's hard to
10:53:32 determine that.
10:53:34 **Q.** Okay. And based on your forensic analysis, was there any
10:53:39 effort to obtain or download a trade secret from that
10:53:43 computer?
10:53:44 **A.** That could not be determined from my analysis. I did
10:53:48 not find evidence of that.
10:53:49 **Q.** Okay. But you did find analysis, did you not, that after
10:53:55 these -- this virus/malware was installed on the computer, was
10:54:03 anything accessed after January 30th?
10:54:09 **A.** I could not determine that from my analysis. I could
10:54:13 not determine that anything was accessed.
10:54:15 **Q.** Okay. So you don't know anything either way?
10:54:18 **A.** No, don't know either way.
10:54:20 **Q.** Now, this computer was also forensically analyzed by the
10:54:29 French Intelligence Service as well; is that correct?
10:54:32 **A.** That is correct.
10:54:32 **Q.** And a report dated September 17, 2014, does that sound
10:54:38 familiar? That was prepared by the French?

10:54:43 **A.** That's probably correct.

10:54:43 **Q.** And do you recall as one of the findings of that report that any data recovery, if any took place, did not appear to be targeted in any matter?

MR. McKENZIE: Objection, Your Honor.

THE COURT: Your objection?

MR. McKENZIE: Objection, Your Honor.

THE COURT: Basis?

MR. McKENZIE: Hearsay.

MS. CORS: Your Honor, I am asking for a finding. I am not asking for him to repeat what was in the report.

THE COURT: Objection's overruled.

You can answer the question, if you remember it.

THE WITNESS: Could you repeat the question, please?

BY MS. CORS:

10:55:22 **Q.** Sure. So as -- was it your understanding that one of the findings of this report was that any data recovery did not appear to be targeted in any manner?

10:55:36 **A.** I don't recall that statement, and I'm a little bit confused on the term "data recovery" being used there. Is that downloading of files, I guess is what my question is?

10:55:53 **Q.** Did you have any understanding as to whether the French forensic analysis concluded that any files were exported?

10:56:03 **A.** I don't believe they could conclude that any files were exported.

10:56:07

10:56:10 **Q.** So it appears, from your perspective, their conclusions
10:56:13 were consistent with the conclusions of your own forensic
10:56:16 analysis?
10:56:17 **A.** That is correct.
10:56:19 **Q.** Now, your report analyzed a file, a self-extracting RAR
10:56:29 file, I believe, that contained images on Mr. Hascoet's
10:56:32 computer; is that correct?
10:56:33 **A.** That is correct.
10:56:35 **Q.** And can you explain to the jury what -- what those images
10:56:38 were?
10:56:39 **A.** The images were pictures of the various locations that
10:56:45 we determined to be in Nanjing, Jiangsu Province.
10:56:52 **Q.** They appeared to be vacation photos?
10:56:55 **A.** They would be consistent with vacation photos.
10:56:57 **Q.** And in the course of your investigation, you reviewed, as
10:57:06 I understand, communications involving Tian Xi, correct?
10:57:11 **A.** Tian Xi, yes.
10:57:13 **Q.** And many of those communications you read here for the
10:57:16 jury, correct?
10:57:16 **A.** That is correct.
10:57:18 THE COURT: Ms. Cors, could you keep your voice up,
10:57:21 please?
10:57:22 MS. CORS: Yes. Sorry, Your Honor.
10:57:23 BY MS. CORS:
10:57:24 **Q.** And in those communications do you recall seeing any

reference to trade secrets?

A. I do not.

Q. Do you recall seeing any discussion about obtaining documents from Safran?

A. I do not.

Q. Do you recall any reference to composite materials?

A. I do not.

Q. Do you recall any reference to aviation technology?

A. I do not.

Q. And do you recall any reference to fan blade technology?

A. I do not.

Q. Okay. And then you were asked to read, and I understand you reviewed, communications involving Mr. Gu Gen, correct?

A. Correct.

Q. And who is Mr. Gu Gen again?

A. Gu Gen is the IT infrastructure and information security officer for Safran Suzhou.

Q. Okay. And with respect to these communications, do these communications reference any effort to obtain documents?

A. They do not.

Q. Do they reference any attempt to steal trade secrets?

A. They do not.

Q. Do they reference any -- do they reference composite materials?

A. No.

10:58:41 **Q.** Do they reference fan blades, including fan blades
10:58:45 designed by GE?
10:58:48 **A.** They do not.
10:58:49 **Q.** Okay. And there were additional communications you were
10:58:51 asked to review and read into the record regarding alleged
10:58:55 colleagues of Mr. Xu, correct?
10:58:59 **A.** That is correct.
10:59:00 **Q.** Chai Meng?
10:59:02 **A.** Chai Meng.
10:59:03 **Q.** And I am going to ask you the same series of questions.
10:59:06 In those communications, was there any reference about
10:59:08 obtaining documents from Safran Suzhou or any entity of
10:59:14 Safran?
10:59:15 **A.** There were not.
10:59:16 **Q.** Were there any reference to trying to obtain trade
10:59:20 secrets?
10:59:20 **A.** There weren't.
10:59:21 **Q.** Any reference to composite materials?
10:59:25 **A.** There was not.
10:59:28 **Q.** Any reference to aviation fan blades?
10:59:34 **A.** No.
10:59:35 **Q.** Or GE Aviation?
10:59:37 **A.** There was not.
10:59:38 **Q.** Now, Mr. Gu Gen was head of security, correct?
10:59:44 **A.** He is head of information security.

10:59:46 **Q.** And in your experience, would someone who's head of
10:59:50 information security have pretty broad access to the databases
10:59:55 and computers of the company?
10:59:57 **A.** Generally, they would.
10:59:59 **Q.** Yet, I believe you just testified there was never a
11:00:01 request of Mr. Gu Gen, to your knowledge, to -- to use that
11:00:05 access to obtain any information from the company, correct?
11:00:08 **A.** Correct.
11:00:09 **Q.** Now, on your direct testimony you talked a little bit
11:00:19 about the MSS and its local office in Nanjing, the JSSD,
11:00:26 correct?
11:00:27 MR. McKENZIE: Objection, Your Honor.
11:00:28 THE COURT: Basis?
11:00:30 MR. McKENZIE: Assumes facts not in evidence.
11:00:32 THE COURT: Sustained as to form.
11:00:40 BY MS. CORS:
11:00:41 **Q.** Mr. James, you were shown documents that the government
11:00:43 alleged related to Mr. Xu, correct?
11:00:47 **A.** Mr. Xu Yanjun.
11:00:52 **Q.** And his alleged role with MSS in its office in Nanjing,
11:00:58 the JSSD, correct?
11:00:59 **A.** I was shown that.
11:01:01 **Q.** The MSS and the JSSD have multiple functions, do they
11:01:15 not?
11:01:16 **A.** They do.

11:01:17 **Q.** Okay. I believe you've testified in the past that in
11:01:20 your view they are sort of a combination of the FBI and CIA,
11:01:25 correct?
11:01:26 MR. McKENZIE: Objection, Your Honor. Outside the
11:01:28 scope of direct.
11:01:32 MS. CORS: May I address this, Your Honor? On
11:01:34 direct, the issue of Mr. Xu and his employment with the MSS
11:01:39 was brought up. On direct the issue of an incursion into a
11:01:44 computer was brought up. I'm simply trying to explore what
11:01:48 could be the basis for an incursion.
11:01:53 THE COURT: The Court overrules the objection. I am
11:01:56 going to give you some latitude.
11:01:58 MR. McKENZIE: Your Honor, I am going to make a
11:02:01 second renewed objection under different grounds of improper
11:02:04 impeachment by referencing prior testimony without asking a
11:02:07 direct question first.
11:02:10 THE COURT: Overruled.
11:02:11 Please proceed.
11:02:14 MS. CORS: Thank you, Your Honor.
11:02:15 BY MS. CORS:
11:02:15 **Q.** Now, with respect to the MSS and the -- let me start with
11:02:19 this.
11:02:20 You had -- in connection with your investigation in the
11:02:25 Southern District of California, did you provide testimony to
11:02:28 the grand jury?

11:02:29 **A.** I did.

11:02:30 **Q.** Okay. And as part of that testimony, did you opine on the roles and functions of the MSS and its office, JSSD and Nanjing?

11:02:41 **A.** Yes.

11:02:41 **Q.** And do you recall identifying some of those functions as somewhat of a combination between the FBI and CIA?

11:02:49 **A.** That would be correct.

11:02:51 **Q.** And you identified one of the primary responsibilities of MSS and JSSD as collecting of intelligence, correct?

11:03:03 **A.** That is correct.

11:03:06 **Q.** Intelligence, by definition information?

11:03:12 **A.** That could be another term for intelligence.

11:03:14 **Q.** It could also include open-source information; is that correct?

11:03:17 **A.** It could.

11:03:18 **Q.** Some of the other functions, I believe you identified nonmilitary foreign intelligence; is that correct?

11:03:24 **A.** That is correct.

11:03:25 **Q.** And then you also identified as a function of both the MSS and the JSSD office performing political and domestic security. Do you recall that?

11:03:37 **A.** I do.

11:03:37 **Q.** And could you explain to the jury what your understanding of political and domestic security is?

11:03:44 **A.** That would be looking for internal spies inside of China.

11:03:51 **Q.** Could it also include monitoring and surveilling foreigners or individuals who are in China?

11:03:56 **A.** It could.

11:03:57 **Q.** Could it also include monitoring and surveilling companies that are operating within China's borders?

11:04:03 **A.** It could.

11:04:06 **Q.** And, in fact, would you agree that China views cyberspace within its national borders as a proper area of control?

11:04:17 MR. McKENZIE: Objection as to first being outside the scope and, second, relevance.

11:04:22 THE COURT: Second, what?

11:04:24 MR. McKENZIE: Relevance as to his opinion.

11:04:29 THE COURT: Overruled.

11:04:31 I'm going to need to break momentarily, but finish up.

11:04:36 MS. CORS: Okay. I can finish this up.

11:04:37 BY MS. CORS:

11:04:38 **Q.** And as part of any functions with respect to political and domestic security, there are a number of methods the Chinese government can use to do that; isn't that correct?

11:04:49 **A.** That is correct.

11:04:50 **Q.** Okay. Do some of those include searching hotel rooms?

11:04:54 **A.** I'm not familiar with exactly what the MSS does or doesn't do inside of China.

11:05:01 **Q.** In terms of monitoring, surveilling, in your experiences
11:05:05 as a cyber expert, could bugging or intruding into someone's
11:05:10 computer to monitor that computer be a technique that --
11:05:14 **A.** That could be.
11:05:15 **Q.** -- is used?
11:05:16 Is that a technique that governments sometimes use to
11:05:18 conduct such surveillance?
11:05:20 **A.** It could be.
11:05:23 THE COURT: I'm going to interject here and ask if
11:05:25 we can break.
11:05:27 MS. CORS: Certainly, Your Honor.
11:05:29 THE COURT: And I think we're straying a bit, but I
11:05:32 gave you some latitude.
11:05:33 Members of the jury, we are going to break for 20
11:05:36 minutes. During the break, take a break. As you know, don't
11:05:39 discuss the case among yourselves or with anyone else. No
11:05:42 independent research. Continue to keep an open mind.
11:05:47 Out of respect for you, we'll rise as you leave for 20
11:05:50 minutes.
11:05:51 THE COURTROOM DEPUTY: All rise for the jury.
11:05:52 (Jury out at 11:05 a.m.)
11:06:31 THE COURT: The jury's left the room. The door is
11:06:34 closed. Is there anything that requires my attention before
11:06:37 we break for 20 minutes? First, from the government?
11:06:41 MR. McKENZIE: No, Your Honor.

11:06:42 THE COURT: From the defense?

11:06:43 MS. CORS: No, Your Honor.

11:06:44 THE COURT: Very well.

11:06:46 Let the record reflect that Judge Cole is here observing my work during recess.

11:06:49

11:06:52 THE COURTROOM DEPUTY: The court is now in recess.

11:06:54 (Recess from 11:06 a.m. until 11:31 a.m.)

11:31:17 THE COURT: May we call for the jury from the government's perspective?

11:31:20

11:31:23 MR. McKENZIE: Yes, Your Honor.

11:31:24 THE COURT: And from the defense as well?

11:31:26 MS. CORS: Yes, Your Honor.

11:31:27 THE COURT: Let's call for the jury. Let me get my mask. You can call for the jury.

11:31:28

11:32:38 THE COURTROOM DEPUTY: All rise for the jury.

11:32:39 (Jury in at 11:32 a.m.)

11:33:10 THE COURT: You may all be seated. Thank you.

11:33:17 The 15 jurors have rejoined us after a break. Thank you for your patience.

11:33:21

11:33:22 We'll continue with the testimony of this witness.

11:33:26 MS. CORS: Thank you, Your Honor.

11:33:30 Your Honor, I have no further questions for this witness. Thank you.

11:33:33

11:33:33 THE COURT: Very well.

11:33:34 Redirect, if any?

MR. McKENZIE: Very briefly, Your Honor.

THE COURT: Very well.

REDIRECT EXAMINATION

BY MR. McKENZIE:

Q. Special Agent James, when you analyzed the Sakula malware, were you able to determine whether or not it beaconed out to a domain?

A. Yes, I was.

Q. Were you able to determine whether any particular files were transferred from the computer to anywhere else?

A. I could not determine that.

Q. Why not?

A. Depending on how the files are transferred, our records are not maintained on the hard drive so it's really hard to determine that after the fact. Generally, you would need to actually watch the transfer occur.

Q. And so just to be clear, is it the case that you determined that no files were transferred, or is it the case that you could not determine what files, if any, were transferred?

A. There was no evidence to support whether or not files were transferred either way.

Q. During your years of experience in cyber intrusion cases involving remote access trojans, is part of the purpose that they're installed to take files?

MS. CORS: Objection, Your Honor.

THE COURT: Basis?

MS. CORS: Leading and beyond the scope.

THE COURT: Overruled.

Don't lead the witness. Go ahead, ask.

BY MR. McKENZIE:

Q. As part of your experience, what are some of the reasons, some of the main reasons that you've experienced for why people installed remote access trojans on computers?

A. Some of the primary reasons are, one, to gain access to the computer so that you can use it to do what your motive is. Once you have access, you can run commands and compromise other computers on the network.

In this case, they used computers that were compromised to compromise other companies.

MS. CORS: Objection, Your Honor.

THE COURT: Beyond the scope?

MS. CORS: Yes, beyond the scope.

THE COURT: Sustained.

MR. McKENZIE: No further questions, Your Honor.

THE COURT: Very well.

Redirect or recross on redirect?

MS. CORS: Thank you, Your Honor.

RECROSS-EXAMINATION

BY MS. CORS:

11:36:38 **Q.** Special Agent James, you just testified that this type of
11:36:42 virus malware can be used to gain access to achieve motives,
11:36:46 correct?
11:36:46 **A.** That is correct.
11:36:46 **Q.** And in this instance, you are not in any position to know
11:36:49 what those motives were, correct?
11:36:54 **A.** Can we be more specific on the question?
11:36:57 **Q.** Well, there can be many different reasons why a person or
11:37:02 entity may seek to install this type of file on a computer,
11:37:07 correct?
11:37:08 **A.** That is correct.
11:37:08 **Q.** And one of those reasons could be to gain access to the
11:37:12 computer and to see what is in the computer to surveil, to
11:37:16 monitor, correct?
11:37:17 **A.** That is correct.
11:37:23 MS. CORS: No further questions. Thank you.
11:37:24 MR. McKENZIE: Nothing further, Your Honor. Thank
11:37:26 you.
11:37:26 THE COURT: Are you going back to San Diego?
11:37:28 THE WITNESS: I hope so.
11:37:30 THE COURT: Travel safe. You may step down, sir.
11:37:33 THE WITNESS: Thank you.
(Proceedings reported but not transcribed.)

CERTIFICATE OF REPORTER

I, Mary A. Schweinhagen, Federal Official Realtime Court Reporter, in and for the United States District Court for the Southern District of Ohio, do hereby certify that pursuant to Section 753, Title 28, United States Code that the foregoing is a true and correct transcript of the stenographically reported proceedings held in the above-entitled matter and that the transcript page format is in conformance with the regulations of the Judicial Conference of the United States.

s/Mary A. Schweinhagen

_____ 15th of December, 2021

MARY A. SCHWEINHAGEN, RDR, CRR
FEDERAL OFFICIAL COURT REPORTER